IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A method for identifying unsolicited electronic mail messages in a computer network, comprising:

receiving an electronic mail message;

removing non-static data including visible end-of-line characters and headers, from the electronic mail message;

generating a checksum based on data remaining within the electronic mail message;

comparing the generated checksum with a database containing checksums for previously identified unsolicited messages; ~~and~~

identifying the electronic message as an unsolicited message if the generated checksum matches one of the database checksums; and

updating the database with new checksums;

wherein the database is updated based on checksums generated from electronic messages received and identified as an unsolicited message;

wherein the non-static data is removed to prevent the non-static data from being subject to the checksum, so that non-static data forged by spammers does not compromise the identification of the electronic message as the unsolicited message.

2. (Cancelled)

3. (Currently Amended) The method of claim [[2]]4, wherein the portions comprise lines of data.

4. (Currently Amended) ~~The method of claim 2~~ A method for identifying unsolicited electronic mail messages in a computer network, comprising:

receiving an electronic mail message;

removing non-static data including visible end-of-line characters and headers, from the electronic mail message;

generating a checksum based on data remaining within the electronic mail message;

comparing the generated checksum with a database containing checksums for previously identified unsolicited messages; and

identifying the electronic message as an unsolicited message if the generated checksum matches one of the database checksums;

wherein the non-static data is removed to prevent the non-static data from being subject to the checksum, so that non-static data forged by spammers does not compromise the identification of the electronic message as the unsolicited message;

wherein generating the checksum comprises generating individual checksums for portions of the remaining data;

wherein comparing [[a]]the checksum comprises comparing checksums starting with one of the portions at the end of the remaining data and working backwards through the data.

5. (Currently Amended) The method of claim 1 wherein removing non-static ~~material~~data comprises removing forwarding information.

6. – 7. (Cancelled)

8. (Original) The method of claim 1 further comprising deleting the electronic mail message if the message is identified as an unsolicited message.

9. (Original) The method of claim 1 further comprising at least temporarily storing the electronic message if the message is identified as an unsolicited message.

10. (Original) The method of claim 1 further comprising forwarding the electronic message to an intended recipient if the message is not identified as an unsolicited message.

11.-14. (Cancelled)

15. (Currently Amended) The system of claim 1[[4]]6 wherein the portions comprise lines of data.

16. (Currently Amended) ~~The system of claim 14~~ A system for identifying unsolicited electronic mail messages in a computer network, comprising:

a message modifier operable to remove non-static data including visible end-of-line characters and headers, from an electronic mail message;

a checksum generator operable to generate a checksum based on data remaining within the electronic mail message;

a database containing checksums previously identified for unsolicited messages; and

a detector operable to compare the generated checksum with the database and identify the electronic message as an unsolicited message if the generated checksum matches one of the database checksums;

wherein the non-static data is removed to prevent the non-static data from being subject to the checksum, so that non-static data forged by spammers does not compromise the identification of the electronic message as the unsolicited message;

wherein the detector is configured to generate individual checksums for portions of the remaining data;

wherein the detector is configured to compare the generated checksums starting with one of the portions at the end of the data and working backwards through the data.

17. (Currently Amended) The system of claim 1[[3]]6 wherein the database is configured to receive updates.

18. (Cancelled)

19. (Currently Amended) The computer product of claim [[18]]21 wherein the computer readable medium is selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, and hard drive.

20. (Cancelled)

21. (Currently Amended) ~~The computer product of claim 20~~ A computer program product for identifying unsolicited electronic mail messages in a computer network, comprising:

code that receives an electronic mail message;

code that removes non-static data including visible end-of-line characters and headers, from the electronic mail message;

code that generates a checksum based on data remaining within the electronic mail message;

code that compares the generated checksum with a database containing checksums for previously identified unsolicited messages;

code that identifies the electronic message as an unsolicited message if the generated checksum matches one of the database checksums;

code that generates individual checksums for portions of the remaining data;

~~further comprising~~ code that compares the generated checksums starting with one of the portions at the end of the data and works backwards through the data; and

a computer readable medium that stores said computer codes;

wherein the non-static data is removed to prevent the non-static data from being subject to the checksum, so that non-static data forged by spammers does not compromise the identification of the electronic message as the unsolicited message.

22. (Original) The method of claim 5 wherein the forwarding information includes a ">" character.

23. (Original) The method of claim 4 wherein the comparing starts with one of the portions at the end of the remaining data and works backwards through the data, in order to reduce required processing.

24. (Original) The method of claim 1 wherein the non-static data is removed prior to the checksum being generated.

25. (Cancelled)